



# THE ESSENTIAL GUIDE TO SINGLE SIGN-ON

Everything You Need to Know to Get Started with SSO

# TABLE OF CONTENTS

- 03 INTRODUCTION
- 04 CHAPTER 1: THE HARD-TO-IGNORE  
FACTS ABOUT PASSWORDS
- 06 CHAPTER 2: HOW SINGLE SIGN-ON  
BENEFITS YOU
- 09 CHAPTER 3: HOW SINGLE SIGN-ON  
BENEFITS YOUR USERS
- 11 CHAPTER 4: HOW SINGLE SIGN-ON WORKS
- 15 CHAPTER 5: SSO FOR CLOUD & MOBILE
- 17 CHAPTER 6: SAY HELLO TO SSO

Download our app. Stay connected with our app. Earn rewards using the app.

It's all about the apps these days. They make it easy for us to get the information we need, do our work and stay connected without being tethered to our desks or computers. Whether web-based apps will ever completely replace locally hosted software is still being debated, but one thing's for sure: apps are here to stay.

It's estimated that the average enterprise already has more than 200 apps in use.<sup>1</sup> While they generally make our lives better and jobs easier, the proliferation of apps also brings challenges. Like managing all of those different login credentials.

**200** apps are in use by the average enterprise<sup>2</sup>

“Man, I wish I had even more usernames and passwords to remember,” said no one ever. And to avoid having to do so, far too many of your users are indulging in [risky password practices](#).

Meanwhile, you're relying on those same flimsy passwords to protect your critical data and resources. To borrow from the popular children's story The Three Little Pigs, relying on passwords alone is like building a straw house. That's a precarious position to be in, especially when the big bad wolf is out there, just waiting to blow your house down.


That may not be the perfect analogy. But don't let that trip you up. The point is this: If you're putting your users in the position of having to create multiple different username and password combinations to access your apps, you're putting your entire enterprise at unnecessary risk.

You'll find a better and more secure approach in single sign-on (SSO). SSO provides [the security your enterprise needs](#), plus the streamlined login and access your users love.

Continue reading to learn everything you need to know about SSO, including:

- Even more reasons to move beyond passwords
- Why implementing SSO benefits you and your users
- The critical difference between basic and federated SSO
- How to secure access to your cloud and mobile apps

<sup>1</sup> 2018 The State of Application Delivery Report, F5 Networks Inc.  
<sup>2</sup> Ibid.

A person wearing a beige, textured sweater is sitting at a desk, typing on a laptop. A clear water bottle is on the desk next to the laptop. The background is slightly blurred, showing a window with a view of trees. The entire scene is overlaid with a dark, semi-transparent filter.

**CHAPTER 1:**  
**THE HARD-TO-  
IGNORE FACTS ABOUT  
PASSWORDS**

The risks of hanging your security hat on passwords is hardly breaking news. By now, everybody and their brother is well aware of what NOT to do when picking passwords. Yet, stolen credentials still top the list of action varieties that lead to data breaches.<sup>3</sup>



still the #1 and #2 worst passwords<sup>4</sup>

Sadly, password practices aren't getting any better. In some ways, they're getting worse. It's estimated that [employees share an average of six passwords](#) with their co-workers, a 50% increase from a year ago.<sup>5</sup> Also, nearly seven out of 10 people are still [reusing the same password](#) across some or all of their online accounts.<sup>6</sup>

These password practices are mind-boggling in an age where identity theft is a very real threat. Even more confusing, almost the same number of people who are reusing passwords also claim to understand what the best practices are (72% to be exact).<sup>7</sup>

But given the explosive growth of web and mobile applications, is it any surprise your users suffer from password fatigue?

**191** the number of passwords the average employee has to manage

A typical employee must keep track of 191 passwords.<sup>8</sup> If that seems high, remember that the average enterprise has 200 applications in use. Even if you prefer conservative estimates, which put the number closer to 30, that's still a heck of a lot of passwords to remember.

The reality is that even those who know better don't always do better. Especially when they're exhausted and searching for an easier way. Your users' password practices are likely the result of managing dozens if not hundreds of login credentials. They're simply looking for some relief. You can give it to them with single sign-on (SSO).

<sup>3</sup> 2018 Data Breach Investigations Report, Verizon.

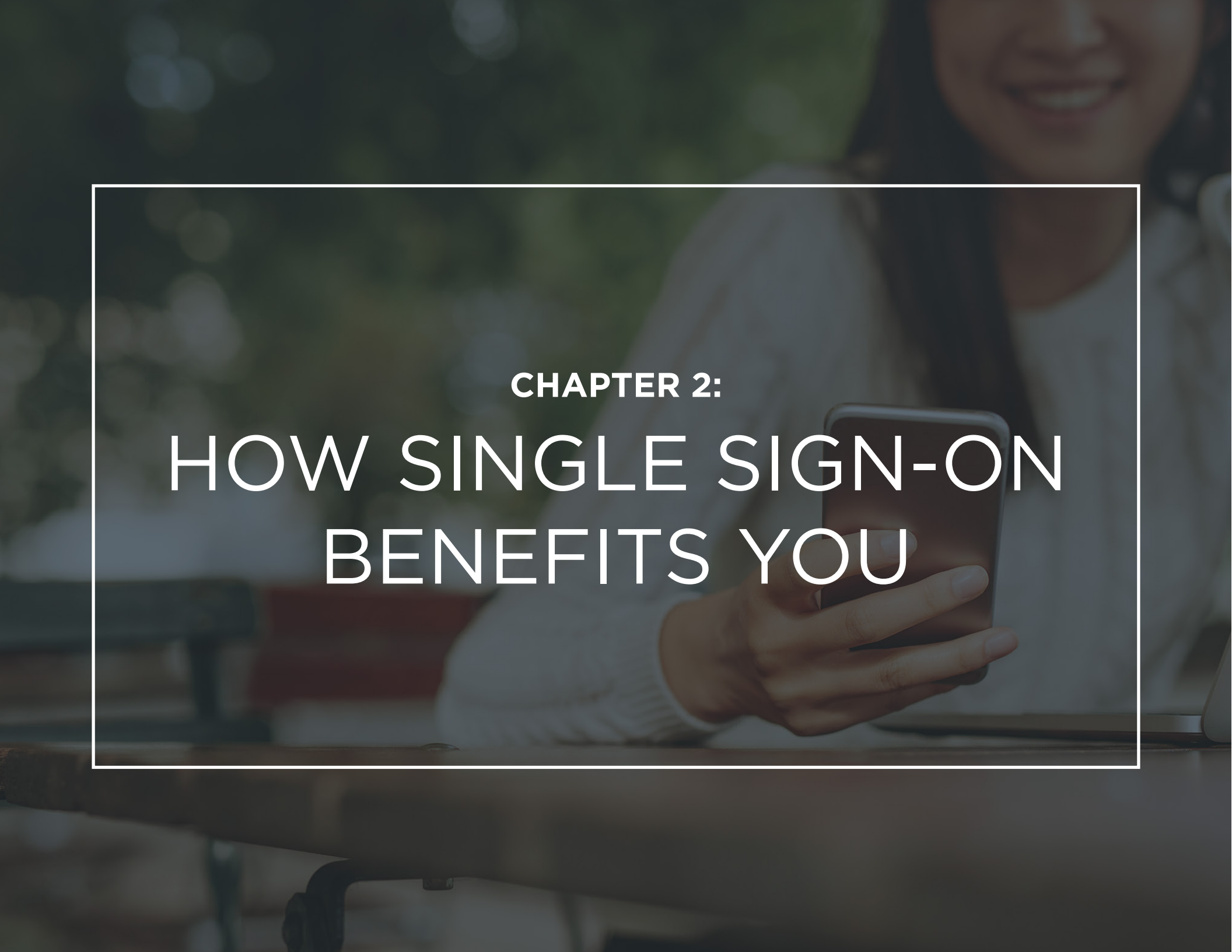
<sup>4</sup> Top 100 Worst Passwords of 2017, SplashData.

<sup>5</sup> 2018 Global Password Security Report, LastPass by LogMeIn.

<sup>6</sup> "How many of your accounts use the same password for online logins?" Statista, Oct 2017.

<sup>7</sup> Ibid.

<sup>8</sup> Ibid.



CHAPTER 2:  
HOW SINGLE SIGN-ON  
BENEFITS YOU

# HOW SINGLE SIGN-ON BENEFITS YOU



Single sign-on eliminates the need for individual passwords for each account and replaces them with a single set of corporate credentials. Your users are able to sign on with just one set of credentials to access all of their applications and services.

In sharp contrast, when you aren't able to use SSO to access resources, you not only have to sign in multiple times, you also need to create sign-on credentials for each app. Making your users manage and remember this many passwords presents obvious security risks to your enterprise.

Some minimize these risks by utilizing techniques like password vaulting and password replay. Password vaults store users' passwords in a directory or password vault, which is usually cloud-based (like LastPass or OneLogin). Password replay retrieves those passwords from the password vault, then replays them to the web application.

These measures may provide a quick fix, but they also pose vulnerabilities. Password vaulting puts all of your passwords at risk. Even if the vault is encrypted, your passwords will be exposed should the vault be compromised. Meanwhile, password replay allows for the risky practice of reusing passwords and puts you at risk of password replay attacks. It also requires synchronization across applications during manual password resets, which is problematic and expensive to maintain.

You'll find a safer solution in federated single sign-on. Federated SSO doesn't just minimize your risks, it delivers five significant advantages to your enterprise.

## 1. Stronger Security

SSO strengthens your enterprise security by reducing the number of passwords your users have to manage. This shrinks the password-attack vector, further reducing the odds of a data breach. Given the average cost of a data breach in 2018 was \$3.86 million,<sup>9</sup> implementing SSO provides a critical safeguard. Your enterprise is able to protect its brand reputation and its bottom line.

## 2. Lower IT Costs

Single sign-on decreases the number of passwords. This translates to fewer help-desk calls for password resets. While a reduction in calls may sound insignificant, consider that several large U.S.-based organizations across different industries are setting aside more than \$1 million each year just for password-related support costs.<sup>10</sup> Eliminating a large percentage of password related help-desk calls could mean significant savings for your enterprise, too.

## 3. Safer Mobile Adoption

Single sign-on provides secure access to apps from any device. Historically, credentials were stored directly on devices. If the device got stolen, so did the user's credentials. But with federated SSO, which uses standard encrypted tokens to share the users' authentication status and identity attributes to facilitate access to applications, credentials are no longer stored on the device. This creates a stronger security posture that facilitates mobile adoption.

## 4. Increased Productivity

It's no secret that providing mobile access to business apps supports workforce productivity. By streamlining and securing access for your users from anywhere on any device, an SSO deployment can drive significant productivity improvements. To put it in a numerical perspective, consider a large, global company that has 20,000 employees logging into an average of five applications per day. If each employee logs into those five applications every day at a rate of 10 seconds per login, the company is losing over 72,000 hours per year of productivity. Think of what your organization can do with an additional 72,000 hours!

## 5. Better User Experience

By providing one-click access to users' apps, SSO eliminates the need to complete redundant sign-on attempts across applications and the frustration of managing multiple passwords. A PwC research study found that 43% of consumers would pay more for greater convenience.<sup>11</sup> A frictionless sign-on experience is one way to provide greater convenience to customers and deliver that same great experience to employees and partners.

<sup>9</sup> 2018 Cost of a Data Breach Study, Ponemon Institute.

<sup>10</sup> Maxim, Merritt and Andras Cser with Stephanie Balaouras, Salvatore Schiano, Madeline Cyr and Peggy Dostie, "Best Practices: Selecting, Deploying, and Managing Enterprise Password Managers," Forrester, Jan 8, 2018.

<sup>11</sup> Clarke, David and Ron Kinghorn, "Experience is everything: Here's how to get it right," PwC, March 26, 2018.



A woman with glasses and a man are looking at a tablet together in an office setting. The woman is pointing at the screen. The background is blurred, showing other people working.

**CHAPTER 3:**

# HOW SINGLE SIGN-ON BENEFITS YOUR USERS

# HOW SINGLE SIGN-ON BENEFITS YOUR USERS

The benefits of SSO don't end at the enterprise. Single sign-on also delivers significant improvements in accessibility and experience to all of your users—whether employees, customers or partners. When enterprises have an [authentication authority](#) with [SSO across everything](#), they can connect any user with any application seamlessly and reduce administrative overhead.

## Employees

For employees, single sign-on enables more convenient enterprise access. This drives improvement in workforce productivity. The time saved by eliminating multiple sign-ons and password resets can easily translate to millions of dollars in savings, too.

[Click here](#) to see how Equinix provides one-click employee access with SSO.

## Customers

Customers demand a fluid user experience. SSO delivers it by streamlining their access to both your internal and third-party apps and resources. This in turn increases app adoption, engagement and loyalty.

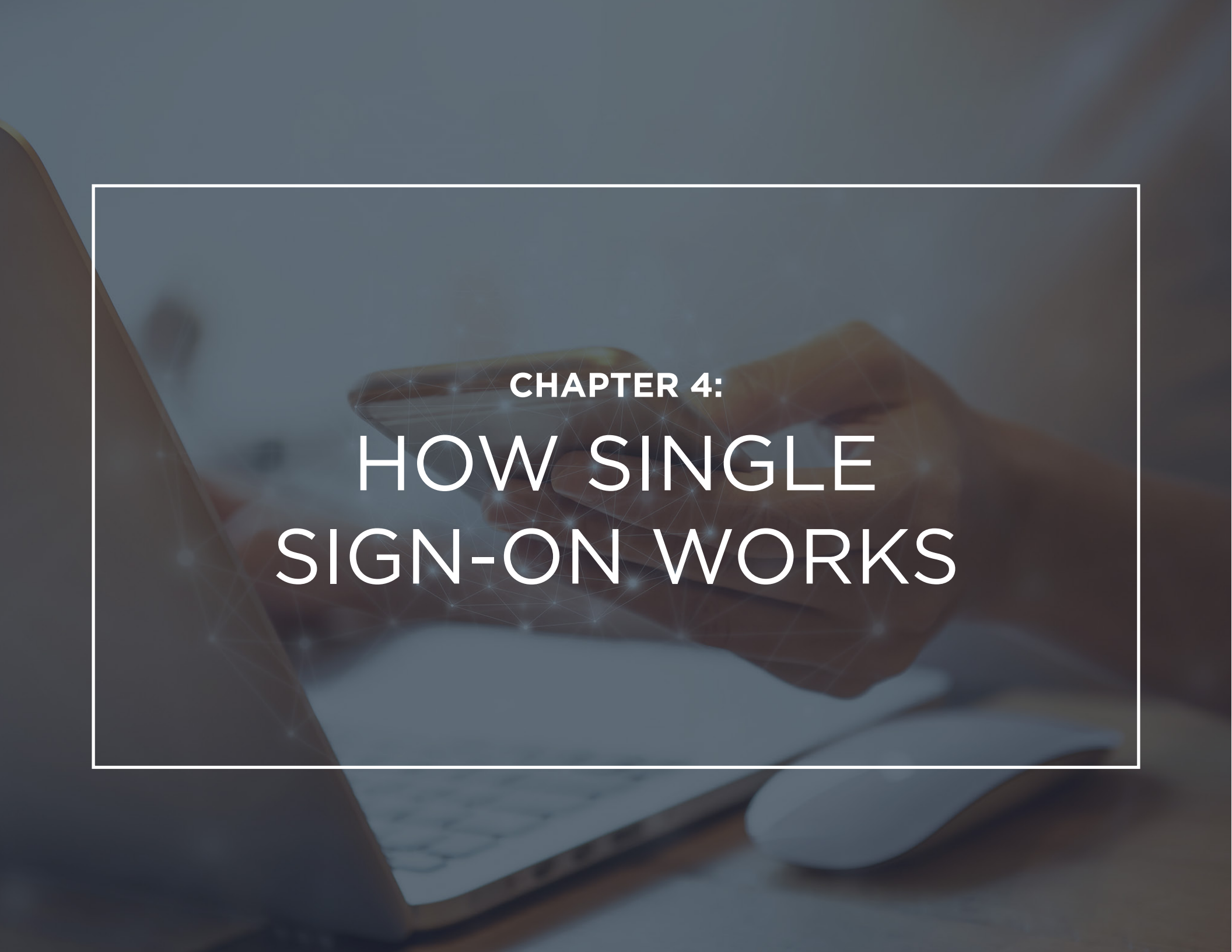
To learn more about the benefits of customer SSO, [get the eBook](#).

## Partners

In today's global economy, partner access is critical. Single sign-on allows you to grant your partners secure access to sensitive data, while making it easy for them to manage and authenticate their own users.

[Click here](#) to learn how to provide partner access the right way with SSO.



A hand holding a smartphone over a laptop keyboard with a network overlay.

CHAPTER 4:  
HOW SINGLE  
SIGN-ON WORKS



The proliferation of on-premises, cloud and SaaS applications is driving the need for enterprises to provide secure single sign-on to a trusted group of applications or “service providers,” even when those resources are owned by third parties or sit outside their firewalls. Federated single sign-on solves this need.

Federation literally means “leagued together” or “allied.” The notion of federation as it relates to sign on—and identity security generally—refers to the ability for a user to authenticate (i.e., prove they are who they say they are) just once and then use that authenticated session to access all of the applications they’re authorized to use, regardless of where those applications reside. As your organization evolves to allow more users to securely access the applications they need, [a single authentication authority](#) that provides SSO across everything becomes essential.

Federated SSO enables authenticated access to applications and systems by securely exchanging user information, even across domains. This requires the establishment of a trust relationship between an organization and an external third party, such as an application vendor or partner, through standard protocols.

Using identity standards like SAML, OAuth, OpenID Connect and SCIM, federated SSO allows for the secure transmission of user access and provisioning information. It does this by using signed assertions or tokens, instead of storing and forwarding usernames and passwords. This practice safeguards web and mobile applications, as well as the APIs that support them.

To effectively connect multiple identity types, today’s large enterprises [deploy an identity federation hub](#), which serves as a bridge to connect all of those user identities in one place.

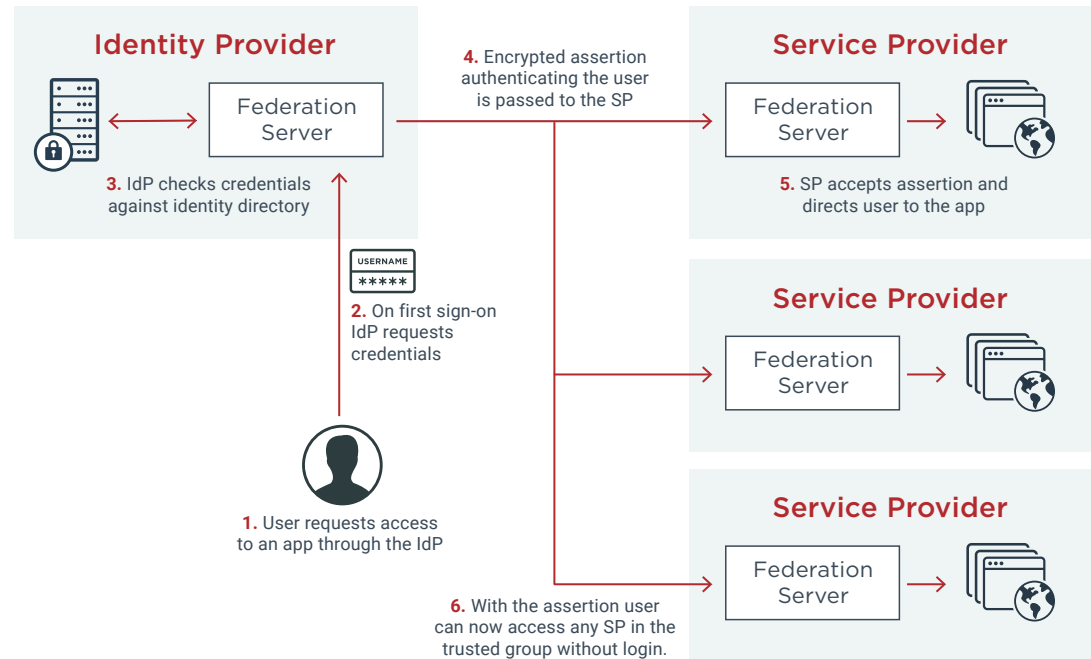
## How Federated SSO Works

First, the organization (known as the identity provider or IdP) must implement a centralized authentication server. This server is then used by all apps to 1) validate a user's identity and 2) issue access tokens, which are encrypted bits of data that confirm the identity and privileges of that user.

During the initial sign on, the user's username and password is directed to the identity provider for verification. The authentication server checks the credentials against the directory where user data is stored. If the credentials check out, the IdP initiates an SSO session on the user's browser.

Once the SSO session is active, the user can access applications from within the trusted group, like a corporate dock. Each time the user requests access to an application, the service provider sends a request to the IdP to authenticate the user's identity. The IdP provides an access token, and the service provider grants access, eliminating the need for additional sign-ons.

## IdP-initiated Federated SSO



The six-step sequence illustrates a typical federated SSO use case.

## Integrating SSO into Existing Environments

To enjoy the advantages of federated SSO, your IAM solution must support [identity standards](#). The use of identity standards reduces the integration efforts between multiple organizations when sharing applications or information. It also brings security to any device, browser or client that is accessing information from applications. To follow are four identity standards you need to know about.

### SAML

Security Assertion Markup Language (SAML) is an open XML standard for exchanging authentication and authorization of data between an identity provider and service provider. SAML allows businesses to safely share identity information across domains (aka federation). [Learn more about SAML.](#)

### OpenID Connect (OIDC)

OpenID Connect (OIDC) adds an identity layer to OAuth 2.0 and simplifies existing federation specifications. It enables identity federation and delegated authorization, plus includes other features and mechanisms that enhance dynamic interoperability. [Learn more about OpenID Connect.](#)


### SCIM

The System for Cross-domain Identity Management (SCIM) uses modern protocols like REST and JSON to reduce complexity and provide a more straightforward approach to user management. The adoption of SCIM allows easier, more powerful and standardized communication between identity data stores.

[Learn more about SCIM.](#)

### OAuth 2.0

The industry-leading standard for enabling access to APIs, OAuth 2.0 provides a standard framework that allows an application to securely access resources on behalf of a user without requiring their password. This open authorization also lets the user understand what kinds of access and information the application is requesting, and then provide consent. [Learn more about OAuth 2.0.](#)

A photograph of two men sitting at a wooden table in a cafe. The man on the left is wearing a dark suit and tie, looking at a tablet held by the man on the right, who is wearing a light-colored shirt and jeans. The background is a brick wall. The image is overlaid with a white border and semi-transparent text.

**CHAPTER 5:**  
**SSO FOR**  
**CLOUD & MOBILE**

## Cloud-based Environments

Amazon Web Services (AWS), Microsoft Azure and Google Cloud are popular cloud environments because they provide anywhere, anytime, any-scale flexibility. However, security risks are greater in the cloud. Federated SSO lets you [integrate identity federation and single sign-on](#) into both your cloud environments and on-premises applications for centralized security, visibility and control of your hybrid IT environment.

Federation and federated SSO provides what are known as the four As of identity security:

1. Authentication
2. Authorization
3. Account management
4. Auditing

In a cloud-based environment, applications must be able to authenticate a user's identity, understand what that user is authorized to do, create or update an account and audit a user's activities. The four As are critical components of an identity security strategy, and provide portability and extensibility beyond enterprise boundaries, making federated SSO essential to the security of a cloud-based environment.

[Click here](#) to learn more about the four As of identity security.

## Mobile Applications

SSO solutions were traditionally limited to providing access to web applications. Unless application providers chose to use the system browser and sacrifice user experience, single sign-on for mobile applications was a difficult prospect.

Today, mobile SSO enables users to sign on once to a secure SSO application on their mobile device and have instant access to all of their enterprise applications. It also solves the problem of having credentials stored on the device itself. With SSO and mobile-based authentication, authentication and authorization is done using standards-based signed assertions or tokens.





CHAPTER 6:  
SAY HELLO TO SSO



It's no secret that passwords don't provide the security they once did. And in today's hyper-connected world, you have more assets and information to protect than ever.

You're also faced with providing access to more users on more devices. No longer content with clunky login requirements, they want one-click access to all of their SaaS, mobile, cloud and enterprise applications.

Single sign-on gives you the strong security you need, while providing the streamlined experience your employees, customers and partners expect. And no one offers more flexibility to meet your SSO needs than Ping.

To learn more about implementing federated SSO in your enterprise, visit [www.pingidentity.com](http://www.pingidentity.com).